



Department of Defense DIRECTIVE

NUMBER 3020.26

September 8, 2004

USD(P)

SUBJECT: Defense Continuity Program (DCP)

References: (a) DoD Directive 3020.26, "Continuity of Operations (COOP) Policy and Planning," May 26, 1995 (hereby canceled)
(b) Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities," November 18, 1988, as amended
(c) Department of Defense Memorandum, "Implementation Guidance on National Security Policy Direction on Enduring Constitutional Government and Continuity of Government Operations," (U) February 17, 1999

1. REISSUANCE AND PURPOSE

This Directive:

- 1.1. Reissues reference (a) and changes its title.
- 1.2. Establishes the Defense Continuity Program (DCP) and the Defense Continuity Executive Steering Group (hereafter referred to as the "Continuity ESG").
- 1.3. Revises continuity policies and assigns responsibilities for developing and maintaining the DCP to enhance the Department of Defense (DoD) readiness posture.
- 1.4. Authorizes publication of additional DoD issuances relating to the DCP and the Defense Continuity Security Classification Guide.

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 1.

4. POLICY

It is DoD policy that:

4.1. The Department of Defense shall have a comprehensive and effective Defense Continuity Program that ensures DoD Component Mission Essential Functions (MEF) continue under all circumstances across the spectrum of threats in accordance with E.O. 12656 and DoD Memorandum, "Implementation Guidance on National Security Policy Direction on Enduring Constitutional Government and Continuity of Government Operations," (U) (references (b) and (c)).

4.2. All Defense continuity-related activities and requirements, to include Continuity of Operations, Continuity of Government, and Enduring Constitutional Government, shall be coordinated under the DCP.

4.3. Performance of MEF in a continuity threat or event shall be the basis for continuity planning, preparation, and execution.

4.4. The DCP plans shall be responsive and executable with little or no warning.

4.5. Adequate resources shall be planned, programmed, and budgeted to meet DCP policies and requirements, as set forth in this Directive. This includes multi-year strategic planning for all assets and resources, and the development, operation, and maintenance of facilities, communications, and transportation capabilities.

4.6. The DCP shall make maximum use of information technology solutions to provide information to leaders and other users, facilitate decision-making, and issue orders and direction.

4.7. A Continuity ESG shall serve the interests of the Secretary of Defense and Chairman of the Joint Chiefs of Staff by providing direction and guidance to the DCP.

4.8. The continuity program in each DoD Component shall be under the management oversight of a senior official who is accountable to the Head of the DoD Component.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Policy shall:

5.1.1. Serve as the DoD single point of contact for continuity-related matters.

5.1.2. Provide strategic guidance and policy direction for, and oversee planning, programming, budgeting, and execution of the DCP.

5.1.3. Provide guidance and oversight for selection of relocation sites for the Secretary and Deputy Secretary of Defense, the OSD Staff, and the DoD Components, in coordination with the Chairman of the Joint Chiefs of Staff and the Director of Administration and Management (DA&M).

5.1.4. Develop and maintain a comprehensive Secretary of Defense continuity plan.

5.1.5. Provide oversight, in coordination with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), for information systems and networks that are critical to performance of MEF during continuity threats or events.

5.1.6. Develop a comprehensive, multi-year continuity test and exercise program to evaluate and validate the readiness of the DCP and DoD Component continuity plans, procedures, and execution. The program shall include collaboration of DCP activities with Federal interagency programs.

5.1.7. Coordinate for Defense Critical Infrastructure Protection and Information Assurance plans and programs to support the execution of MEF.

5.1.8. Develop, coordinate, and promulgate prioritized and validated requirements for use of DoD transportation assets in support of emergency evacuation and crisis-related operations in the National Capital Region (NCR).

5.1.9. Develop continuity security classification guidance in accordance with governing Executive orders and DoD Directives.

5.1.10. Ensure operations security (OPSEC) requirements are integrated into continuity planning, execution, and operations.

5.1.11. Charter and administer the Continuity ESG, and designate a senior official to co-chair the Continuity ESG in accordance with the charter.

5.1.12. Represent the Department of Defense in Federal interagency continuity matters as required, and coordinate Defense continuity planning and activities with national continuity and homeland security efforts.

5.2. The Heads of the DoD Components shall:

5.2.1. Develop, coordinate, and maintain continuity plans, and shall validate, update, and reissue plans every 2 years, or more frequently as changes warrant. Plans shall:

5.2.1.1. Identify and prioritize organizational MEF.

5.2.1.2. Define emergency delegations of authority and orders of succession for key positions; identify and provide for alert/notification, movement, and training of continuity staffs; and address information technology and communications support to continuity operations.

5.2.1.3. Identify relocation sites or platforms for Component use during continuity threats or events. Site selection should consider geographical dispersion, and maximize co-location and dual-use facilities.

5.2.1.4. Provide for the identification, storage, protection, and availability for use at relocation sites, the vital records, materiel, and databases required to execute MEF.

5.2.1.5. Outline a decision process for determining appropriate actions in implementing continuity plans and procedures with or without warning, during duty and non-duty hours, and address the stand-down of continuity operations and transition back to normal operations.

5.2.2. Develop and implement coordinated, multi-year strategic management plans for assets and resources in support of the DCP, as appropriate.

5.2.3. Ensure that continuity programs are adequately planned, programmed, and budgeted, and that DCP-unique requirements are specifically identified in their budgets. This shall include all assets and resources and the development, maintenance, and operations of facilities, communications, and transportation capabilities.

5.2.4. Integrate continuity-related functions and activities into operations and exercises to assure that MEF can be performed across the spectrum of continuity threats or events.

5.2.5. Test and exercise continuity plans at least annually, or as otherwise directed, to evaluate program readiness.

5.2.6. Integrate OPSEC requirements into continuity planning, execution, and operations.

5.2.7. Identify a senior official to manage, oversee, and ensure readiness and compliance of the Component continuity program with the policies and responsibilities set forth herein.

5.2.8. Designate a representative to the Continuity ESG standing membership in accordance with the Continuity ESG Charter, as appropriate.

5.3. The Under Secretary of Defense for Acquisition, Technology, and Logistics shall identify policy and provide guidance to the DoD Components, as necessary, on the integration of continuity requirements in the research, development, acquisition, and logistical support of equipment, systems, and facilities.

5.4. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall aggregate information on DoD Component funding programmed and budgeted to support the DCP.

5.5. The Under Secretary of Defense for Intelligence shall:

5.5.1. Ensure intelligence support to the DoD Components.

5.5.2. Oversee intelligence collection and analysis programs supporting the DCP.

5.5.3. Ensure threat and warning information is properly disseminated to support decision-making regarding continuity activities.

5.5.4. Develop, in coordination with the Under Secretary of Defense for Policy (USD(P)), intelligence and geospatial information requirements for support of continuity staffs.

5.5.5. Coordinate the development of an annual evaluation of foreign intelligence collection and terrorist threats against the DCP.

5.5.6. Ensure the continuity readiness of the Defense Intelligence components.

5.6. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer shall:

5.6.1. Incorporate DoD continuity capabilities into the integrated command and control enterprise.

5.6.2. Validate Defense Continuity Integrated Network (DCIN) requirements through the Pentagon Area Common Information Technologies Services, Executive Board in coordination with the USD(P) and the DA&M.

5.6.3. Oversee information systems and networks that are critical to the performance of MEF during continuity threats or events.

5.6.4. Determine requirements for additional commercial and Federal communication services and facilities to support the execution of MEF during a crisis.

5.7. The Director of Administration and Management shall:

5.7.1. Manage the OSD Continuity of Operations Information Technology Program for OSD relocation sites.

5.7.2. Serve as the program manager for the DCIN-Pentagon Continuity Information System.

5.8. The Director, Washington Headquarters Service shall:

5.8.1. Exercise overall management responsibility for the Raven Rock Military Complex. This includes management of all facility infrastructure operations, renovation, capital improvements, and common information technology infrastructure and services. In exercising this responsibility, appropriate consultation and coordination shall be accomplished with the Commander, Military District of Washington, the Army CIO/G6, the Continuity ESG, and Site R tenants.

5.8.2. Exercise overall responsibility for OSD relocation sites in the NCR. This includes management of all facility infrastructure operations, renovation, capital improvements, and common information technology infrastructure and services.

5.9. The Chairman of the Joint Chiefs of Staff shall:

5.9.1. Provide the DoD Components with designated combat or combat support roles, planning guidance on defense continuity matters pertaining to those roles.

5.9.2. Assure the survivability, reliability, and availability of command and control systems comprising the National Military Command System (NMCS) at relocation sites and across the spectrum of contingency situations.

5.9.3. Ensure the Combatant Commanders address the readiness status of command and control systems and command centers that support the NMCS.


5.9.4. Develop and maintain an overarching operations plan for use of DoD transportation assets in support of emergency evacuation and crisis-related operations in the NCR, and provide guidance and direction to the DoD Components providing assets on plan implementation and execution.

5.9.5. Designate a senior official to co-chair the Continuity ESG.

5.10. The Secretaries of the Military Departments shall support emergency evacuation and crisis-related operations in the NCR in accordance with the Chairman of the Joint Chiefs of Staff NCR emergency evacuation operations plan.

6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 1

E1. Definitions

E1. ENCLOSURE 1

DEFINITIONS

E1.1.1. Continuity of Government (COG). A coordinated effort within each Branch of Government ensuring the capability to continue Branch minimum essential responsibilities in a catastrophic crisis. COG is dependent on effective continuity of operations plans and capabilities. DoD COG activities involve ensuring continuity of DoD MEF through plans and procedures governing succession to office; emergency delegations of authority (where permissible, and in accordance with applicable law); the safekeeping of vital resources, facilities, and records; the improvisation or emergency acquisition of vital resources necessary for the performance of MEF; and the capability to relocate essential personnel and functions to, and sustain performance of MEF at, alternate work site(s) until normal operations can be resumed.

E1.1.2. Continuity of Operations (COOP). An internal effort within individual components of the Executive, Legislative, and Judicial Branches of Government assuring the capability exists to continue uninterrupted essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies. COOP involves plans and capabilities covering the same functional objectives of COG, must be maintained at a high level of readiness, and be capable of implementation both with and without warning. COOP is not only an integral part of COG and Enduring Constitutional Government (ECG), but is simply "good business practice" - part of the Department of Defense's fundamental mission as a responsible and reliable public institution.

E1.1.3. Crisis. An incident or situation involving a threat to the United States, its territories, citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, political, or military importance that commitment of U.S. military forces and resources is contemplated to achieve national objectives.

E1.1.4. Critical Infrastructure Protection (CIP). The identification, assessment, and security of physical and cyber systems and assets so vital to the Nation that their incapacitation or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety. Within the Department of Defense, it is the identification, assessment, and security enhancement of physical and cyber assets and associated infrastructures essential to the execution of the National Military Strategy. Defense CIP is a complementary program linking the mission assurance aspects of Anti-Terrorism, Force Protection, Information Assurance, Continuity of Operations, and Readiness programs.

E1.1.5. Defense Continuity Executive Steering Group (Continuity ESG). Senior representatives from designated OSD Components, Joint Staff, Military Services, and Defense Agencies that serve as the "board of directors" for the DCP to provide guidance and oversight for DoD continuity-related activities, while developing and implementing a DoD-wide continuity strategy for the twenty-first century threat environment. The Continuity ESG also adjudicates functional disputes concerning the use of common DoD continuity resources that support the Secretary of Defense and the Chairman of the Joint Chiefs of Staff.

E1.1.6. Defense Continuity Integrated Network (DCIN). The DoD enterprise-wide means used to ensure availability of mission-critical information to support Secretary of Defense and Chairman of the Joint Chiefs of Staff MEF during continuity contingencies.

E1.1.7. Defense Continuity Program (DCP). An integrated program comprised of defense policies, plans, procedures, assets, and resources that ensures continuity of DoD Component MEF under all circumstances, including crisis, attack, recovery, and reconstitution. It encompasses the DoD Components performing Continuity of Operations, Continuity of Government, and Enduring Constitutional Government functions across the spectrum of threats to continuity.

E1.1.8. Enduring Constitutional Government (ECG). A cooperative effort among the Executive, Legislative, and Judicial Branches of Government, coordinated by the President, to preserve the capability to execute constitutional responsibilities in a catastrophic crisis. ECG is the overarching goal; its objective is the preservation of the constitutional framework under which the Nation is governed. ECG requires orderly succession and appropriate transition of leadership, and integrated performance of essential functions by all three Branches of Government. ECG is dependent on effective COOP and COG capabilities.

E1.1.9. Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E1.1.10. Mission Essential Functions (MEF). The specified or implied tasks required to be performed by, or derived from, statute or Executive order, and those organizational activities that must be performed under all circumstances to achieve DoD Component missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly impact DoD ability to provide vital services, or exercise authority, direction, and control.

E1.1.11. National Capital Region (NCR). The geographic area located within the boundaries of the District of Columbia; Montgomery and Prince Georges Counties in the State of Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties and the Cities of Alexandria, Fairfax, Falls Church, Manassas, and Manassas Park in the Commonwealth of Virginia; and all cities and other units of government within the geographic areas of such District, Counties, and Cities.

E1.1.12. National Security Emergency. Any occurrence including, but not limited to, natural disaster, military attack, technological failures, civil unrest, or other disruptive condition that seriously degrades or threatens the national security of the United States.